Electronic Frontier Canada
La Frontière Électronique du Canada

Comments Regarding

the Consultation Paper on Digital Copyright Issues

I. Executive Summary

Electronic Frontier Canada, joined by the parties noted below, submit these comments in response to the Consultation Paper on Digital Copyright Issues ("Consultation Paper") prepared by the Intellectual Property Directorate of Industry Canada and the Copyright Policy Branch of Canadian Heritage (the "Departments"). These comments will address two of the four proposed Copyright Act amendments considered in the Consultation Paper: (1) legal protection for technological measures; and (2) the liability of network intermediaries.

With respect to any contemplated circumvention measures, we urge the Departments to protect two important Canadian public policies: (1) the historical balance between the interests of the public and copyright owners, as reflected in the rights and exceptions contained in the Copyright Act; and (2) the public values of free expression and scientific progress, reflected in the section 2(b) of the Canadian Charter of Rights and Freedoms. In light of these concerns, we make the following recommendations:

Proposal 1: Reconsider whether any changes to the Copyright Act are required by the WIPO Copyright Treaty.

Proposal 2: Any circumvention prohibition should be limited to circumventions undertaken for the purpose of infringement.

Proposal 3: Any circumvention prohibition should include a "legitimate purpose" exception.

Proposal 4: Any circumvention prohibition must include protections for "innocent circumventors."

Proposal 5: Circumvention prohibitions should reach only acts of circumvention, and should not include prohibitions on devices and technologies that can be used for legitimate circumvention activities.

With respect to any limitations on copyright liability for network intermediaries, we urge the Departments to be ensure that any such safe harbors: (1) create a regime that respects the privacy and free expression rights of Internet

users; and (2) preserve and foster the end-to-end architecture that has made the Internet such an successful platform for innovation and competition. In light of these goals, we make the following recommendations:

Proposal 1: No affirmative obligation to monitor Internet users.

Proposal 2: Notice and take-down should be limited to materials residing on the ISP's own computer systems.

Proposal 3: Notice and take-down procedures should reasonably preserve user anonymity.

Proposal 4: Any notice and take-down process should include a non-waivable affirmative counter-notice provision in favor of Internet users.

Proposal 5: Anyone performing ISP functions, including the transmission and routing of network transmissions, hosting or caching, should be entitled to whatever safe harbor is ultimately adopted.

II. The Commenting Parties

These comments reflect the views of and are submitted by the following organizations:

Electronic Frontier Canada (La Frontière Électronique du Canada): Electronic Frontier Canada (EFC) is Canada's premier online civil liberties organization, and is devoted to the protection of fundamental rights and freedoms as new computing, communication, and information technologies are introduced into Canadian society. EFC's activities are national in scope. EFC is a federally incorporated non-profit organization and was founded in January 1994 by Professor David Jones (McMaster University), Professor Jeffrey Shallit (University of Waterloo), and Professor Richard Rosenberg (University of British Columbia). All board members hold Ph.D's in computer science or related fields. EFC's several hundred supporting members are drawn from all Canadian provinces and territories, and from a diversity of backgrounds, ages, and professions. EFC maintains an interactive online presence with its supporting membership through its electronic discussion list EFC-TALK@efc.ca and its web site http://www.eff.ca/.

Electronic Frontier Foundation: The Electronic Frontier Foundation is the leading civil liberties organization devoted to protecting individual rights in the digital world. Founded in 1990, EFF actively encourages and challenges industry and government to support free expression, privacy, and openness in the information society. EFF is a private, nonprofit, member-supported organization based in San Francisco, California, U.S.A., and maintains one of the most linked-to websites in the world: http://www.eff.org.

OpenCola, Ltd.: With offices in Toronto and San Francisco, OpenCola (www.opencola.com) is Canada's leading, funded peer-to-peer (P2P) software company. Founded in 1999, OpenCola is developing an application suite to allow users to create automated networks that act as collaborative filters, capturing the

decisions of each user in the system to create automatic recommendations for files and resources.

ColdStream Associates Ltd.: A Canadian owned and operated management consulting firm that specializes in advanced information security. Our activities include and have included in the past: security audit, InfoSec architecture, policy & procedure, internal audits, privacy issues, defence and forensics. Our clients include a number of multinational corporations and other large organizations who require high end information security services. Additional information can be found at http://coldstream.ca/.

Sandelman Software Works: Sandelman Software Works was formally founded in 1996 by Michael Richardson after a number of years of less formal work. Based in Ottawa, Ontario, Sandelman Software Works does consulting and contracting in TCP/IP networking and Unix systems. The company has done work in network design, network security and network security products. While security is the primary focus, systems internals (specifically device drivers) and software/hardware interfaces are secondary areas of expertise. Additional information can be found at http://www.sandelman.ottawa.on.ca/.

TransGaming Technologies Inc.: TransGaming Technologies is an innovative Canadian software startup working on multimedia software portability technology for new platforms such as the Linux operating system. TransGaming's work makes it possible for Linux users to play their favourite Windows games directly on their Linux systems. TransGaming believes strongly in the need for well thought out internet-oriented copyright legislation that preserves the principals of fair dealing and does not alter the delicate balance between the rights of copyright holders and the rights of individuals and society at large.

FLORA Community Consulting and Community Web: FLORA Community Consulting <http://www.flora.ca/> is a business operating out of Ontario, Canada which focuses on solutions based on Open Source and/or Free Software based computing. FLORA.org Community Web <http://www.flora.org/> is an independently owned and operated volunteer service that acts as part of the Community Networking movement. FLORA.org is primarily concerned with freedoms such as free speech and free software. Activities involve the hosting of alternative viewpoints such as alternative (to the private automobile) transportation, alternative education (home-schooling, etc), alternative politics (Green Parties), and alternative economics (Free Software's philosophical alternative to "ideas as industrial-era property").

III. Legal Protection of Technological Measures

With respect to proposed legal protections for technological measures, the 1996 World Intellectual Property Organization (WIPO) Copyright Treaty requires that signatories provide "adequate legal protection and effective legal remedies against circumvention of effective technological measures that are used by

authors in connection with the exercise of their rights."[1] Any implementing legislation, however, must respect two important Canadian public policies: (1) the historical balance between the interests of the public and copyright owners, as reflected in the rights and exceptions contained in the Copyright Act; and (2) the public values of free expression and scientific progress, reflected in the section 2(b) of the Canadian Charter of Rights and Freedoms. International experiences with "anti-circumvention" provisions suggests that they must be implemented with caution and restraint, lest these important Canadian values be undermined.

A. Preservation of the Copyright Balance

As the Consultation Paper recognizes, Canada's Copyright Act is premised on "a balance between the rights of creators and the interests of users."[2] Because this balance aims to reconcile important competing public policy priorities, the crafting of the copyright balance has properly rested in the hands of the Canadian legislative and judicial process, and is "the outcome of extensive debate, consultation, jurisprudence and legal obligation."[3]

The balance is reflected in the Copyright Act by a broad grant of certain exclusive rights to copyright owners for a limited time, on one hand, and a number of exceptions and limitations to preserve access for the public, on the other. Each of the limitations on the scope of a copyright owner's exclusive rights reflect a deliberate legislative conclusion that public policy imperatives outweigh the interest in maximizing incentives for copyright owners. For example, several elements of the Copyright Act reflect a recognition of the critical roles played by libraries, archives and museums in ensuring that a repository of knowledge and culture remains accessible to all citizens.[4] The public's side of the balance also includes "fair dealing," which includes the right to make uses of copyrighted works for research or private study without fear of unwanted scrutiny from copyright owners.[5] Other provisions recognize the special needs of educational institutions[6] and individuals with perceptual disabilities.[7] Many of these exceptions were enacted as recently as 1997, after the lengthy deliberations resulting in *An Act to Amend the Copyright Act* (Bill C-32). The Copyright Act further recognizes the principle that ideas and facts are not the proper subject of copyright, and that in certain circumstances the public must be permitted to access these unprotected elements even when they are embedded within copyrighted works.[8]

---

[1] 1996 WIPO Copyright Treaty, Article 11. *See also* Article 18 (relating to performers or producers of phonograms).

[2] Consultation Paper, at 22.

[3] Id. at 23.

[4] Copyright Act, sec. 30.1, 30.2, 30.3.

[5] Copyright Act, sec. 29. *See also* sec. 29.1 (fair dealing for purpose of criticism or review); 29.2 (fair dealing for purpose of news reporting).

[6] Copyright Act, sec. 29.4, 29.5, 29.6, 29.7, 30.3.

[7] Copyright Act, sec. 32.

[8] *See generally* Gammon, "The Legal Protection of Ideas" (1991), 29 Osgoode Hall L.J. 93.

The adoption of broad anti-circumvention provisions could supplant entirely this careful copyright balance in the digital realm, replacing it with a one-sided legal regime that accommodates only the interests of rights holders. The danger from overly broad anti-circumvention protections is plain: if rights holders are entitled to prohibit circumvention and circumvention devices generally, they are able to prohibit what the Copyright Act would otherwise permit. For example, under an overly-broad anti-circumvention provision, a use that would otherwise be permitted as "fair dealing" under the Copyright Act would no longer be permissible with respect to a technologically protected work. Suddenly, the vitality of "fair dealing," an important element of the copyright balance, would depend entirely on unilateral decisions by copyright owners.

An overly broad circumvention ban would also effectively undo the exceptions carefully crafted by the legislature as part of the 1997 *Act to Amend the Copyright Act* (Bill C-32). For example, section 32 of the Copyright Act specifically provides that a person may, at the request of a blind person, make a copy of a literary work in a format that can be read by the blind. However, if a literary work were released in a technologically protected form (such as an Adobe eBook), the exercise of the statutory right would likely require both an act of circumvention and the availability of circumvention tools, both of which would be prohibited by a broad circumvention ban.

The role of libraries could also be dramatically altered in a world of technologically protected works. Library patrons may someday find themselves faced with row upon row of pay-per-use works secured by technological protection measures. Broad anti-circumvention provisions would prohibit librarians from tampering with the restrictions imposed by copyright owners. Absent some right to circumvent, coupled with access to circumvention tools, the library will have been transformed from a repository of public knowledge into a glorified rental outlet.

The risk posed by overly-broad circumvention provisions is that copyright law, with its mixture of rights and exceptions, would be supplanted by circumvention law. The copyright balance, instead of being crafted by elected representatives and the judiciary, would be dictated entirely by the private decisions of copyright owners. This result cannot be reconciled with the historical balance reflected by Canadian copyright law.

Early experience with the broad anti-circumvention provisions enacted in the United States bear out these concerns. As noted in the Consultation Paper, in 1998 the U.S. enacted the Digital Millennium Copyright Act (DMCA). The DMCA includes broad prohibitions on both acts of circumvention and circumvention devices.[9] In *Universal City Studios v. Reimerdes*, a number of major motion picture companies brought suit against *2600* magazine for publishing a software program, known as DeCSS, that defeats the CSS encryption scheme used to protect movies on DVDs. One defense raised by *2600* turned on the fact that DeCSS could be used to facilitate “fair use,” a doctrine long-

[9] *See* 17 U.S.C. § 1201.

established in U.S. copyright law. The court rejected this defense, reasoning that the statutory exceptions to copyright had no application to violations of the DMCA's broad anti-circumvention provisions.[10] In effect, the court held that the use of technological protection measures on DVDs trumped the legislatively-crafted copyright balance set forth in the U.S. Copyright Act.

New digital technologies will certainly pose new challenges for copyright owners. They will also pose challenges for those who otherwise would enjoy the benefit of legislatively-crafted exceptions to the Copyright Act, as they encounter an increasing number of copyrighted works that are protected by technological measures. These challenges, however, do not justify the wholesale abandonment of Canada's historical copyright balance in favor of technological controls unilaterally adopted by copyright owners. The balancing approach embraced by the Copyright Act has proven flexible enough to adapt to technological change in the past, and there is no reason to believe that it cannot continue to adapt. As the Consultation Paper recognizes, the creation of prohibition on circumvention would create a new layer of protection for copyright owners. If such a new protection is viewed as necessary, it should be subject to at least the same limitations that apply to a copyright owner's other exclusive rights.

B. Freedom of Expression and Scientific Research

Section 2(b) of the Canadian Charter of Rights and Freedoms recognizes that everyone should enjoy "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication." In considering any proposed circumvention ban, the desire to grant additional protections to copyright owners must be tempered by serious consideration of this fundamental freedom. In particular, the freedoms of scientists and programmers to conduct research and publish their results may be threatened by overly-broad circumvention prohibitions.

Experience with the DMCA's anti-circumvention provisions in the United States illustrate the threat posed by broad circumvention prohibitions to free expression generally, and to scientific research in particular. As discussed in the Consultation Paper, the DMCA imposes a broad prohibition on both acts of circumvention and "any technology, product, service, device, component, or part thereof" that is used to circumvent technological measures that protect copyrighted works.[11] By sweeping an entire category of "technologies" into its "device" ban, the DMCA has effectively created a class of "forbidden knowledge," chilling a variety of publishers and scientists.

The *Universal City Studios v. Reimerdes* case illustrates the chilling effect that overly-broad circumvention prohibitions can have on the freedom of the press. As discussed above, in that case *2600* magazine published the DeCSS computer code as primary source material in the course of its ongoing coverage of

[10] *See Universal City Studios v. Reimerdes*, 111 F.Supp.2d 294, 324 (S.D.N.Y. 2000).

[11] 17 U.S.C. § 1201.

the controversy surrounding the DMCA.[12] Notwithstanding the guarantee of freedom of the press secured by the U.S. Constitution's First Amendment, a court permanently enjoined the magazine from publishing the information, and further enjoined it from publishing links to other locations from which the information could be obtained.[13] In effect, the copyright owners in that case obtained a "stop the presses" order against the publication of truthful materials by a news publication covering a matter of public concern. The implications of such an outcome in Canada would certainly implicate section 2(b) of the Charter.

Copyright owners in the U.S. have also used the DMCA to block the publication of scientific research. In a case that has received considerable media attention, Princeton Professor Edward Felten and a team of researchers have been forced to file suit against a number of music industry entities after being threatened with DMCA liability for trying to present a scholarly paper at an academic conference.[14] Representatives of the Secure Digital Music Initiative (SDMI) claimed that the paper, which explained how Felten's team had defeated watermarking technology meant to protect digital music, was a circumvention technology prohibited by the DMCA.[15] Only after the Felten team filed a lawsuit did SDMI representatives back down from their earlier threats.[16]

Perhaps the most troubling application of the DMCA is the recent criminal prosecution of Russian programmer Dmitry Sklyarov. Sklyarov's employer, a Russian software company known as Elcomsoft, produced and distributed software that can be used to convert digital books from Adobe's eBook format into Adobe's PDF format. In the course of the format conversion, the use restrictions imposed by the eBook format are stripped away. It is undisputed that the Elcomsoft software can be used to facilitate noninfringing uses of eBooks (e.g., fair use excerpting, or to facilitate automated translation into Braille for blind readers). Sklyarov himself was never accused of infringing a copyright, or assisting in the infringing activities of any third party. Nevertheless, for his part in developing the software, U.S. officials arrested him and held him in custody for 3

---

[12] Although Canadian law is not well-developed on this point, it should be clear that computer code, when used expressively, comes within the reach of section 2(b) of the Charter. Numerous U.S. courts that have examined whether computer code should come within the U.S. constitutional guarantee of free expression have concluded that such code can be expressive, and that when used expressively, is entitled to protection as speech. *See Junger v. Daley*, 209 F.3d 481, 485 (6th Cir.2000); *Bernstein v. U.S. Dept. of Justice*, 176 F.3d 1132, 1141, *reh'g granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir.1999); *Universal City Studios v. Reimerdes*, 111 F.Supp.2d 294, 326 (S.D.N.Y. 2000); *Bernstein v. U.S. Dept. of State*, 922 F.Supp. 1426, 1436 (N.D.Cal.1996) (First Amendment extends to source code).

[13] *Universal City Studios v. Reimerdes*, 111 F.Supp.2d 294 (S.D.N.Y. 2000).

[14] *See* Declan McCullagh, "Code Breakers Go to Court," *Wired News* (June 6, 2001) <http://www.wired.com/news/mp3/0,1285,44344,00.html>.

[15] *See* Letter from Matthew Oppenheim to Prof. Edward Felten, April 9, 2001 <http://cryptome.org/sdmi-attack.htm>.

[16] *See* Declan McCullagh, "SDMI Code Breaker Speaks Freely," *Wired News*, August 16, 2001 <http://www.wired.com/news/politics/0,1283,46097,00.html>.

weeks.[17] He and Elcomsoft were recently indicted by a grand jury in San Jose, California. Based on the indictment, Sklyarov faces a maximum of 25 years in prison and a fine that could exceed $2 million.[18]

These three cases have cast a pall on a variety of publishers, innovators, scientists, and organizers of scientific conferences. For example, online service providers have begun to censor message board postings that discuss technological protection measures for fear of incurring DMCA liability.[19] Programmers have withdrawn computer security products from the marketplace and have been reticent to reveal security weaknesses in existing digital rights management (DRM) technologies.[20] Sony has used the DMCA to crack down on an innovative potential competitor who offered a software emulator that permits Apple Macintosh users to play Playstation videogames without the use of a Playstation game console.[21] Prominent non-U.S. computer security researchers have expressed concerns regarding travel to the United States in light of the DMCA, and one researcher has refused to release his research for fear of future U.S. prosecution.[22] Russia has gone so far as to issue an official travel advisory warning programmers of the risks of prosecution in the United States under the DMCA's anti-circumvention provisions.[23]

These anecdotes indicate not only an impairment of the freedom of expression, but also suggest that overly broad circumvention protections may backfire, undermining the very science of computer security on which technological protection measures depend. It is by attacking technological protection measures and reporting the results that the science of computer security moves forward. If circumvention prohibitions deter security experts from testing protection systems, these systems will necessarily be less secure in the long run.[24] This outcome disserves not only the interests of science, but also the interests of

---

[17] *See* Professor Larry Lessig, "Jail Time in the Digital Age," *N.Y. Times* (July 30, 2001) http://www.nytimes.com/2001/07/30/opinion/30LESS.html>; Declan McCullagh, "Hacker Arrest Stirs Protest," *Wired News* (July 19, 2001) <http://www.wired.com/news/politics/0,1283,45342,00.html>; Jennifer 8 Lee, "U.S. Arrests Russian Cryptographer as Copyright Violator," *N.Y. Times*, July 18, 2001.

[18] *See* Brad King & Michelle Delio, "Sklyarov, Boss Plead Not Guilty," *Wired News* (Aug. 30, 2001) <http://www.wired.com/news/politics/0,1283,46396,00.html>.

[19] Lisa M. Bowman, "TiVo Forum Hushes Hacking Discussion," *CNET News* (June 11, 2001) <http://news.cnet.com/news/0-1005-200-6249739.html> (censorship of discussion of video extraction software); John Borland, "Sega Wants to Silence Advice on Hacker Sites," *CNET News* (Oct. 4, 2000) < http://news.cnet.com/news/0-1005-200-2931893.html>.

[20] Robert Lemos, "Security Workers: Copyright Law Stifles," *CNET News* (Sept. 6, 2001).

[21] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Technology L.J. 519, 556 (1999), available at <http://www.sims.berkeley.edu/~pam/papers.html>.

[22] Lisa M. Bowman, "Researchers Weight Publication, Prosecution," *CNET News* (August 15, 2001) <http://news.cnet.com/news/0-1005-200-6886574.html>.

[23] Jennifer 8 Lee, "Travel Advisory for Russian Programmers," *N.Y. Times* (Sept. 10, 2001).

[24] National Research Council, The Digital Dilemma: Intellectual Property in the Digital Age (2000), at 311-30 (Appendix G describing methods of cryptology research).

the copyright owners who rely on protection systems to safeguard their copyrighted works.

C. Proposals

In light of the important public policy concerns discussed above, we propose the following:

Proposal 1: Reconsider whether any changes to the Copyright Act are required by the WIPO Copyright Treaty.

Changes to the Copyright Act may not be necessary in order to comply with the WIPO Copyright Treaty. The exclusive rights granted to copyright owners by the Copyright Act may already provide the "adequate legal protection and effective legal remedies" required by the Treaty. For example, most illegitimate circumvention activity will necessarily result in an unauthorized reproduction, and hence be subject to traditional copyright sanctions. In addition, to the extent copyright owners are concerned that circumvention will lead to widespread distribution of their works over the Internet, such unauthorized distribution would likely constitute copyright infringement under existing Canadian copyright laws, whether as unauthorized reproductions or communications to the public.

We are aware that Johanne Daniel and Lesley Ellen Harris concluded that specific circumvention legislation was required in their July 1998 "Discussion Paper on the Implementation of the WIPO Copyright Treaty." In light of intervening developments, however, it may be appropriate to revisit this question. In particular, it does not appear that Daniel and Harris considered whether the rights of reproduction and communication to the public adequately protect copyright owners who utilize technological protections. Their report also failed to consider whether the obligations of the WIPO Copyright Treaty are (or should be) addressed by legislation aimed at computer tampering, rather than in the Copyright Act.

Proposal 2: Any circumvention prohibition should be limited to circumventions undertaken for the purpose of infringement.

In the event the Departments conclude that implementing legislation is necessary, and that such legislation should take the form of an anti-circumvention provision in the Copyright Act, we propose that such a provision be made expressly subject to the exceptions contained in the Copyright Act. This goal can be accomplished by prohibiting the circumvention of technological protection measures for infringing purposes, where such measures have been adopted to restrict acts not permitted by the Copyright Act.[25]

[25] This approach was presented as a proposal in both the Consultation Paper and the Discussion Paper by Daniel and Harris. See Consultation Paper at 24; Discussion Paper at 6. This approach was also proposed during the U.S. consideration of the DMCA. See H.R. 3048, 105th Cong. (introduced by Rep. Boucher and Campbell, Nov. 13, 1997).

An anti-circumvention provision of this sort would accommodate the principle of balance embodied in the Copyright Act. For example, an act of circumvention would not be prohibited where undertaken for the purpose of engaging in activities permitted under the Act, including those activities authorized by the statutory exceptions applicable to "fair dealing," libraries, educational institutions, museums, and organizations that assist the perceptually disabled.

Proposal 3: Any circumvention prohibition should include a "legitimate purpose" exception.

Any circumvention prohibition should also include an express exception permitting circumvention where undertaken for legitimate purposes. In arguing for prohibitions on acts of circumvention and circumvention devices, the copyright industries have understandably focused on movies, music, books and other traditional objects of copyright law. The use of technological protections in the digital realm, however, implicates public policy concerns reaching beyond those addressed by the Copyright Act. Trade secret owners, privacy-seeking individuals, and network administrators, to name a few, are already deploying technological protection measures. Email traffic, for example, is entitled to protection under the Copyright Act as literary works. Assuming that privacy-seeking individuals begin to encrypt their email, would a network administrator be entitled to circumvent such encryption to examine their contents? What if the examination were limited to seeking out harmful computer viruses attached to email messages? These questions cannot be answered solely by the application of copyright law principles, but necessarily involve a consideration of privacy, computer security, and other public policies.

As technological protection measures are deployed in an increasing number of unforeseen contexts, the Copyright Act will increasingly become an ill-fitting straight-jacket for courts and policy-makers. Accordingly, a "legitimate purpose" exception will be necessary if the judiciary is to retain the flexibility to consider public policy issues beyond those addressed in the Copyright Act.[26] It is bad enough that circumvention provisions might supplant the copyright balance; without a "legitimate purposes" exception, circumvention provisions threaten to supplant other carefully crafted legal regimes, as well.

Proposal 4: Any circumvention prohibition must include protections for "innocent circumventors."

In order to offset the chilling effect created by uncertain circumvention rules, monetary and criminal penalties for circumvention should be reserved for cases where the unlawfulness of the activity in question is clearly established. Defendants operating in good faith on uncertain legal terrain ("innocent circumventors") should face, at most, only injunctive penalties.

---

[26] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Technology L.J. 519, 543-46 (1999) (discussing need for "legitimate purposes" exception), available at <http://www.sims.berkeley.edu/~pam/papers.html>.

As the Consultation Paper recognizes, "rules that are unclear may have a chilling effect on legitimate uses of works that are nonetheless permitted under copyright law."[27] As a result, circumvention provisions should be drafted so as to give clear notice to citizens regarding which activities are forbidden. However, because the circumvention provisions are likely to have application in areas unforeseeable today, some uncertainty regarding the precise scope of any circumvention prohibition will likely persist. A limitation of liability for "innocent circumventors" would reduce the chilling effect of such uncertainty. It would also decrease the chilling effect of over-reaching threats by copyright owners (such as the threats leveled at Professor Felten and his research team in the U.S.). This, in turn, will increase the likelihood that novel cases will be resolved by the courts, and clarifying the law for the future.

Courts could look at numerous factors in determining whether a circumventor had undertaken circumvention activities, later determined to be unlawful, under a good faith belief that they were lawful. Factors could include whether previous judicial or regulatory pronouncements clearly established that the activity in question constituted unlawful circumvention, and whether the circumventor had reasonably relied on the opinion of counsel.

Proposal 5: Circumvention prohibitions should reach only acts of circumvention, and should not include prohibitions on devices and technologies that can be used for legitimate circumvention activities.

As discussed above, a well-crafted circumvention provision should (1) only apply to activities undertaken with the purpose of copyright infringement; and (2) should be subject to a "legitimate purposes" exception. If these limitations are to have any practical meaning, the public must have access to technologies and devices that will enable legitimate circumvention activities.

The difficulty then becomes distinguishing tools designed to aid legitimate circumvention from those that facilitate unlawful circumvention. This task is likely to be impossible. The very same capabilities that can be used for legitimate purposes can generally also be used for illegitimate ones. In this regard, circumvention technologies and tools are no different from the VCR, photocopiers, and audio recorders, each of which can be used for infringing or noninfringing activities.

It should be noted that copyright owners are not without recourse against technology manufacturers and distributors, even in the absence of circumvention device prohibitions. The exclusive right to “authorize” the exercise of any of a copyright owner’s exclusive rights will continue to protect the interests of copyright owners against technology vendors who knowingly facilitate copyright infringement by third parties.[28]

---

[27] Consultation Paper, at 13.

[28] *See Canadian Cable Television Assn. v. Canada (Copyright Board)* (1993), 46 C.P.R. (3d) 359 at 372 (Fed. C.A.), *leave to appeal refused without reasons* (1993), 51 C.P.R. (3d) v (S.C.C.).

In addition, it is clear that the 1996 WIPO Copyright Treaty does not *require* the adoption of device restrictions. During the negotiation of the Copyright Treaty, in fact, a device-oriented approach was specifically rejected, and replaced with the more general "adequate protection" language that became Article 11.[29]

If the Departments conclude that a device prohibition is necessary, we submit that such a restriction should be narrowly limited to devices whose sole use is to perform unlawful circumvention. In other words, such a restriction should be limited to purpose-built "black boxes" that lack any legitimate use. In addition, for the reasons discussed above in connection with freedom of expression and scientific research, any such restriction should be narrowly tailored to reach only self-contained, fully-functional devices intended for distribution for profit. Scientific methods, ideas, algorithms, research reports, and any noncommercial software code should be expressly carved out of any device prohibition.

IV. Intermediary liability

The Consultation Paper contains several proposals aimed at addressing the question of copyright liability for network intermediaries, including Internet service providers (ISPs). We endorse the Departments' efforts to craft clear rules that will clarify the murky state of the law regarding the copyright responsibilities of network intermediaries. However, in addition to balancing the interests of rights holders and the ISP community, we believe that any solution to the question of ISP liability must also take the interests of the public into account. In particular, any copyright liability solution designed to assist network intermediaries should satisfy the following criteria: (1) it should create a regime that respects the privacy and free expression rights of Internet users; and (2) it should preserve and foster the end-to-end architecture that has made the Internet such an successful platform for innovation and competition.

A. Privacy and Free Expression

The Internet affords individuals and institutions an unprecedented opportunity for free expression at a relatively low cost. Numerous network intermediaries, however, act as gatekeepers to the fora for free expression online. For example, most Internet users rely on an ISP for network access, and may rely on a variety of other service providers for web hosting, instant messenging, message boards, email and access to newsgroups. Accordingly, although the Internet provides remarkable opportunities for free expression, an Internet user's ability to partake of those opportunities depends on her relationship to a variety of network intermediaries. Network intermediaries are also in a position to directly influence the level of privacy that an Internet user enjoys. ISPs generally know the identities of their subscribers and have the ability to monitor all incoming and

[29] *See* Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 Va. J. Int'l Law 369, 409-15 (1997).

outgoing network traffic.[30] In light of these realities, it is crucial that any regime addressing the copyright liability of ISPs provide incentives that reinforce, rather than undermine, the free expression and privacy rights of Internet users.[31]

B. The End-to-End Internet Architecture

The Internet has not only created unprecedented new opportunities for inexpensive speech, but has also proven to be a remarkable incubator for innovation. Any regime aimed at limiting the copyright liabilities of network intermediaries should, to the extent possible, preserve and foster the rapid innovation that has characterized the Internet thus far.

Stanford Law School's Professor Larry Lessig has written extensively regarding the way in which one architectural feature of the Internet is largely responsible for its innovative character.[32] Professor Lessig refers to this feature as the "end-to-end" principle—the notion that the network itself should remain "stupid" (i.e., unable to discriminate between different forms of network traffic), while "intelligence" should be distributed to its "ends" (i.e., on the computers of end-users). Although this architectural principle was originally adopted for technical reasons, it soon became clear that it also entailed certain social and economic consequences. For example, the end-to-end principle by its nature fosters free expression, as it limits the extent to which network owners can discriminate between favored and disfavored content passing through its wires.

In addition, the end-to-end principle, by enforcing competitive neutrality, has profound consequences for innovation. Anyone with a new idea can rely on the fact that the network will treat her applications the same way that it treats competing applications introduced by the largest corporations. In contrast to the communications infrastructures that preceded it, such as telephone and cable television, the end-to-end architecture of the Internet creates an "innovation commons," an open, level playing field that permits innovators to compete on equal footing. The result has been an enormous explosion of innovative uses for the Internet.

Any limitation of liability that may be crafted for network intermediaries should be careful to foster, rather than undermine, the end-to-end principle. In particular, any legal structures that would place ISPs and other network

---

[30] Users can, by employing cryptography, proxy servers, and creating secure "tunnels" between computers, take steps to make surveillance of their communications more difficult. Nevertheless, just as we do not place the burden on telephone users to stop eavesdropping by the telephone company, we should also protect the privacy of the less sophisticated Internet user.

[31] Limitations of liability for copyright infringement should also extend equally to any indirect liability for circumvention that may arise as a result of subscriber activities.

[32] *See* Larry Lessig, The Future of Ideas: the Fate of the Commons in a Connected World (forthcoming October 2001); Larry Lessig, "Innovation, Regulation, and the Internet," *The American Prospect*, v. 11, issue 10 (March 27-April 10, 2000), available at <http://www.prospect.org/print-friendly/print/V11/10/lessig-l.html>; Larry Lessig & Mark Lemley, In re Transfer of Control of Licenses from MediaOne Group, Inc. to AT&T Corp. (testimony before the FCC regarding open access), available at <http://cyberlaw.stanford.edu/lessig/content/testimony/cable/lem-lesd.pdf>.

intermediaries in a privileged position vis-a-vis other Internet users would appear to violate the end-to-end principle. Similarly, any legal structure that creates incentives for ISPs to monitor and discriminate between different types of content would seem to threaten the innovation commons.

Proposal 1: No affirmative obligation to monitor Internet users.

In light of the principles discussed above, we support the Departments' conclusion that a limitation of liability for ISPs should not be conditioned on an affirmative obligation to monitor the activity of its users. Not only would such a system be burdensome on ISPs, it would violate the reasonable expectations of Internet users. Just as we do not expect that our telephone calls will be monitored by the telephone company, nor that our mail will be read by the letter carrier, so to should Internet users be able to rest easy in the knowledge that their every message is not being monitored for copyright infringement. In addition, a regime that requires monitoring would require that ISPs build a monitoring infrastructure that would discriminate among different users and content types. Such an infrastructure would undermine the end-to-end nature of the Internet.

Proposal 2: Notice and take-down should be limited to materials residing on the ISP's own computer systems.

We also support the Departments' conclusion that notice and take-down should be limited to materials hosted or cached on the ISP's own computing equipment, and should not apply to materials stored on an Internet user's own computer. The combination of "always on" broadband Internet connectivity and increasingly powerful personal computers will likely result in an increase in the number of Internet users who host their own Internet content. This development, in turn, is likely to result in a more diverse, decentralized ecosystem of affordable Internet technologies and content, and should be encouraged. To the extent an ISP is providing only simple network connectivity, rather than storing content on behalf of its subscribers, copyright law should not create an incentive for it to monitor or intrude into the computer systems of its subscribers.

Proposal 3: Notice and take-down procedures should reasonably preserve user anonymity.

Anonymous speech has long played a crucial role in fostering free expression. From the pseudonyms used by the authors of the Federalist Papers in the colonial United States to the anonymous criticisms of Chinese communist rulers published in world newspapers in the 1980s, authors of politically sensitive publications have long relied on anonymity to protect their identities and sometimes even their lives. Similarly, anonymity protects "whistleblowers" reporting on government or business abuses or violations of law. A cloak of anonymity may also be crucial for victims of domestic violence or child abuse, and others who want to discuss sensitive, personal information without fear of reprisal or exposure. All of these situations occur daily on the Internet and all of them are worthy of some modicum of protection. This is not to say that Internet users are entitled to anonymity in all circumstances. But, by the same token, the public's right to speak anonymously ought not be overlooked on the Internet.

In the U.S., the ability of ISPs to unmask anonymous Internet users has proven to be a weakness in the protection of freedom of expression. Companies angered by critical comments on public message boards, for example, have found that they can easily file a civil suit, issue a subpoena to the ISP hosting the discussion, and obtain the identity of the speaker. These subpoenas have effectively stifled discussion in many public forums. The situation is even worse where allegations of copyright infringement are concerned. Under the DMCA's safe harbor provisions, a copyright owner is entitled to issue a subpoena to a service provider in order to obtain the identity of an anonymous Internet user. This subpoena can be issued even where the copyright owner has no intention of filing an infringement action—a take-down notice is enough to entitle a copyright owner to a subpoena. A service provider that receives such a subpoena, moreover, is not under any obligation to inform the subscriber that identifying information has been released.

We recommend that the Departments omit subpoena provisions from any ISP safe harbor provisions that it may recommend. A notice and take-down procedure adequately provides to copyright owners the equivalent of an automatic injunction against alleged infringers. If a copyright owner requires additional information regarding an anonymous Internet infringer, the owner can file suit avail itself of the ordinary judicial process, and require that the ISP disclose identifying information. There is no reason that copyright owners should be accorded a special right to breach the legitimate anonymity rights of Internet users upon the submission of a mere allegation of infringement. In addition, we recommend that an obligation be imposed on network intermediaries (including ISPs) to notify a subscriber when his or her identity has been requested by a third party.

Proposal 4: Any notice and take-down process should include a non-waivable affirmative counter-notice provision in favor of Internet users.

Any notice and take-down regime should include a non-waivable counter-notice provision in favor of Internet users. In the absence of such a provision, the free expression rights of individuals are likely to be at the mercy of unscrupulous copyright owners intent on stifling critical speech rather than protecting their works. For example, a corporate copyright owner intent on silencing a critical web site might deliver a take-down notice to the hosting ISP. In order to preserve its eligibility for the copyright liability safe harbor, the ISP will likely respond by taking down the site. As a result, a naked allegation would effectively entitle a copyright owner to the equivalent of permanent injunctive relief. The site owner, meanwhile, would effectively have been silenced without the benefit of any judicial process at all.[33] This concern is not merely hypothetical—there have been reported accounts in the U.S. of the DMCA's notice and take-down provisions being used to shut down web sites under circumstances that suggest that the

[33] The site operator could, of course, transfer the web site to another ISP. There is no guarantee, however, that the copyright owner would not deliver a take-down notice to this ISP as well.

copyright owner was responding to the site's critical message, rather than any infringement.[34]

In order to prevent abuses of the notice and take-down process, a counter-notification process should be put in place for users who want to contest a take-down notice. Under such a system, a subscriber would be notified of the ISP's receipt of a take-down notice, and would have the option, within a short time, of submitting a counter-notice under penalty of perjury disputing the allegation of copyright infringement. If the ISP receives the counter-notice within the relevant counter-notice period, it would forward a copy to the complaining party and would be relieved from any take-down obligation. At that point, the complaining party would be free to file suit against the subscriber directly. In order to further deter abusive take-down notices, a subscriber should be entitled to recover attorneys fees and costs in any case where a court concludes that the original take-down notice was sent in bad faith.

In the U.S., the DMCA provides for a counter-notice procedure similar to the one detailed above. The U.S. provision, however, suffers from two serious flaws. First, it does not address whether an ISP is required to implement the counter-notice procedure, or whether it can instead avoid the obligation by obtaining a contractual waiver from its subscribers as part of its standard "terms of service" agreement. It appears that most ISPs in the U.S. include provisions in their contractual agreements that render the counter-notice provisions of the DMCA safe harbors optional, at best. Obviously, to the extent the implementation of a counter-notification procedure might increase costs to an ISP, the ISP may prefer to obtain contractual waivers in place of a counter-notice regime. Such an outcome, however, would render the counter-notice provisions an empty promise. Accordingly, any contractual efforts by ISPs that purport to waive the counter-notification process should be expressly pre-empted.

The second weakness of the DMCA's counter-notice provisions is that it provides that a take-down is effective immediately upon notice, and remains effective for a 10-day period even in the face of a counter-notice. This arrangement transforms a simple allegation of infringement into an automatic gag order, an outcome that fails to protect the free speech interests of the web site publisher. A 10-day gag order, moreover, renders the counter-notice process substantially less useful to a subscriber, since moving the disputed content to another ISP may provide a more timely solution. Thus, instead of deterring abusive take-down notices and the resolution of disputed infringement claims by judicial inquiry, the U.S. counter-notice provisions encourage an inefficient game of whack-a-mole, as the subscriber shuttles from ISP to ISP in order to elude the draconian effect of abusive take-down notices.

---

[34] *See* Katharine Mieszkowski, "No Free Speech for Animal Rights Web Sites," *Salon* (Aug. 31, 2001) (British medical research company uses DMCA notices to silence critical animal rights web sites) <http://www.salon.com/tech/log/2001/08/31/dmca_animals/index.html>.

Proposal 5: Anyone performing ISP functions, including the transmission and routing of network transmissions, hosting or caching, should be entitled to whatever safe harbor is ultimately adopted.

Any limitation of liability for ISPs should extend equally to anyone performing the functions of an ISP. To the extent the Consultation Paper suggested that such limitations of liability should be reserved for "respectable, accountable" ISPs, we urge the Departments to reconsider its approach.

The rollout of "always on" broadband Internet connectivity, along with increasingly powerful PC hardware and software, has resulted in a recent renaissance for the "end-to-end" principles that have spurred Internet growth and innovation. Already, the sorts of activities once reserved for sophisticated systems administrators and online service providers (such as hosting a web site, having remote access to your home PC while traveling, and providing web services such as email to other Internet users) have become available to the average home Internet user.[35] Dramatically more "intelligence" is becoming available at the "ends" of the network. If this trend is permitted to flourish, a new wave of innovation is likely to emerge, as average Internet users become better able to participate in the networked world as a "peer," contributing services to the Internet community as well as consuming them. For example, individual Internet users have begun organizing grassroots wireless networks built on inexpensive 802.11b technology.[36] When these individuals provide network connectivity to their community, they are acting in exactly the same capacity as an ISP, and should be entitled to the same legal protections from copyright liability.

Restricting a limitation of liability to a category of incumbent ISPs, while withholding these same advantages from average Internet users who will increasingly be able to perform ISP functions, is likely to severely compromise end-to-end architecture principles. We urge the Departments to ensure that all Internet actors, whether large ISPs or individual Internet users, will play on a level copyright playing field when providing identical services to third parties.

****

Electronic Frontier Canada and the other signatories to these comments thank you for your consideration.

Professor David Jones
Electronic Frontier Canada
Dept of Computer Science
McMaster University

---

[35] Apple's recently introduced MacIntosh operating system, OS X, now includes Apache web server software, a powerful server once the province of sophisticated server operators. This software, which runs some of the largest e-commerce sites in the world, now ships standard on every MacIntosh, including the colorful, entry-level iMac.

[36] *See* Damien Cave, "Unchaining the Net," *Salon* (Dec. 1, 2000) <http://www.salon.com/tech/feature/2000/12/01/wireless_ethernet/index.html>.

1280 Main St West
Hamilton, ON L8S 4K1
http://www.efc.ca/
djones@efc.ca
+1 (905) 525-9140 ext.24689 (telephone)
+1 (905) 524-0340 (facsimile)